

Taras Kick (Cal. Bar No. 143379)
taras@kicklawfirm.com
Tyler Dosaj (Cal. Bar No. 306938)
tyler@kicklawfirm.com
THE KICK LAW FIRM, APC
815 Moraga Drive
Los Angeles, CA 90049
Tel: (310)395-2988 / Fax: (310)395-2088

Daniel H. Charest (*pro hac vice*)
dcharest@burnscharest.com
Darren Nicholson (*pro hac vice*)
dnicholson@burnscharest.com
Chase Hilton (*pro hac vice*)
chilton@burnscharest.com
BURNS CHAREST, LLP
900 Jackson Street, Suite 500
Dallas, TX 75202
Tele: (469)904-4550 / Fax: (469)444-5002

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

JOSE GUZMAN, FORTINO RUTILO
JIMENEZ, BERTHA MEZA, GRISELDA
AVILES CARRILLO and JOSE GERARDO
VALLEJO PEREZ individually and on behalf
of all others similarly situated,

Plaintiffs,

v.

WESTERN UNION FINANCIAL SERVICES
INC., MONEYGRAM PAYMENT
SYSTEMS, INC., DOLEX DOLLAR
EXPRESS, INC., and FORCEPOINT LLC.

Defendants.

Case No.: 5-24-cv-00404-SSS-
DTB

CLASS ACTION

**FIRST AMENDED CLASS
ACTION COMPLAINT FOR**

- (1) Violation of the California
Consumer Privacy Rights
Act § 1798.150 *et seq.*; and
(2) Invasion of Privacy,
California Constitution Art.
1, § 1.

DEMAND FOR JURY TRIAL

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, Bertha Meza, Griselda Aviles Carrillo, and Jose Gerardo Vallejo Perez on behalf of themselves and all others similarly situated, by and through undersigned counsel, file this First Amended Class Action Complaint against Western Union Financial Services, Inc. (“Western Union”), MoneyGram Payment Systems, Inc. (“MoneyGram”), and Dolex Dollar Express, Inc. (“Dolex”) (collectively, “Money Transfer Defendants”). Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, Bertha Meza, Griselda Aviles Carrillo, and Jose Gerardo Vallejo Perez on behalf of themselves and all others similarly situated, also bring this Class Action Complaint against Forcepoint LLC (“Forcepoint” or “Database Defendant”).

NEED FOR ACTION

1. The Money Transfer Defendants are in the business of providing money transfer services to individual consumers, typically across international borders. As part of these services, they are entrusted with the personal information of their consumers. Much to their consumers’ detriment, that trust is wholly unwarranted. As detailed below, the Money Transfer Defendants in coordination with the Database Defendant voluntarily participated and continue to participate in a massive and unlawful data dragnet collection and dissemination operation that compromises the personal information of millions of unsuspecting consumers. Defendants’ outrageous conduct is contrary to their express legal obligations and their stated commitment to protecting sensitive consumer information.

//

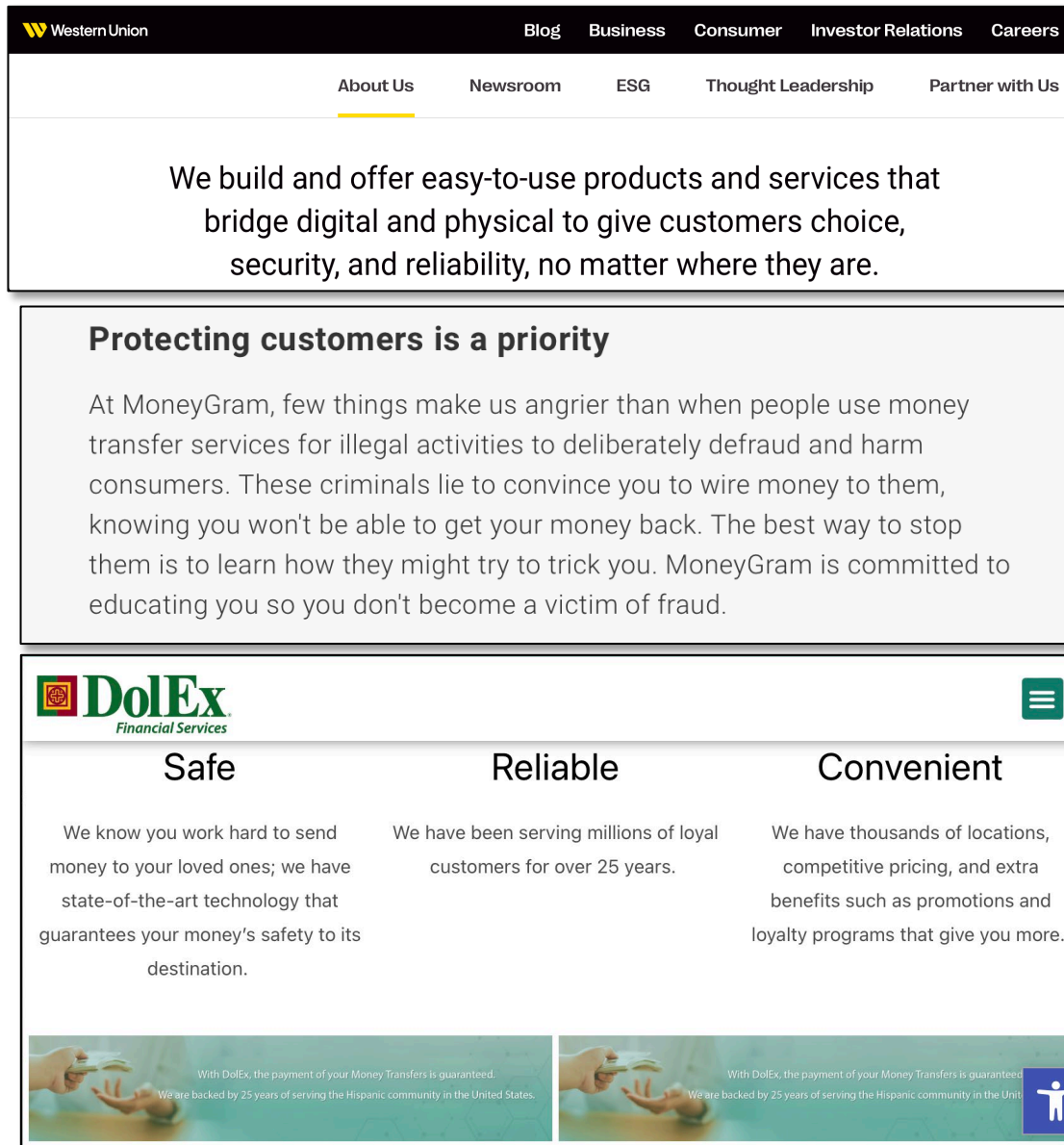
//

//

//

//

2. Indeed, each Money Transfer Defendants' website emphasizes their commitment to the privacy of the services they provide, stating things such as:



¹ <https://corporate.westernunion.com/> (last visited February 12, 2024).

² <https://www.moneygram.com/mgo/us/en/help/fraud-aware/fraud-prevention-information/> (last visited February 12, 2024).

³ <https://www.dolex.com/money-transfer/> (last visited April 10, 2024).

1 3. On January 15, 2023, the American Civil Liberties Union publicly
2 released documents showing that Western Union and MoneyGram, in conjunction
3 with state and federal actors, actively took part in a massive and unlawful dragnet
4 data collection scheme to disclose their own consumers' personal information
5 ("Protected Personal Information" as defined in Cal. Civ. Code §
6 1798.81.5(d)(1)(A)) to private actors, specifically Transaction Record Analysis
7 Center, Inc. ("TRAC") and Forcepoint.

8 4. This unlawful data dragnet operation swept up Protected Personal
9 Information related to Money Transfer Defendants' consumers who sent or received
10 \$500 or more between Arizona, California, California, New Mexico, Texas, and the
11 country of Mexico.

12 5. The Protected Personal Information that Money Transfer Defendants
13 collected and disclosed was never sent to law enforcement. Instead, it was sent to
14 TRAC, an Arizona non-profit corporation whose tax filings indicate its stated
15 mission is: "[t]o educate law enforcement and industry to money laundering
16 technique and trends." The Protected Personal Information was sent via Forcepoint.

17 6. As revealed in the ACLU press release, the Money Transfer Defendants
18 engaged in a years-long data dragnet collection and dissemination operation
19 premised on facially improper "administrative subpoenas" sent by the Arizona
20 Attorney General that cast an impermissible breadth and depth. In 2007, the Arizona
21 Court of Appeals found the Arizona Attorney General was improperly using the
22 administrative statute and that these types of "administrative subpoenas" were
23 invalid and illegal. These administrative subpoenas are just as invalid and illegal
24 today as they were in 2007.

25 7. Likewise, the Money Transfer Defendants' data dragnet collection and
26 dissemination operation was also premised upon facially improper U.S. Immigration
27 and Customs Enforcement, Homeland Security Investigations ("HSI") "customs
28

1 summonses,” which HSI withdrew after Senator Ron Wyden shined light on this
2 utterly invasive surveillance sweep on unsuspecting consumers.

3 8. After the Money Transfer Defendants gave Plaintiffs’ Protected
4 Personal Information to TRAC, TRAC used its database vendor Forcepoint to
5 receive and ingest the Protected Personal Information before allowing law
6 enforcement agencies around the country unfettered access to this Protected Personal
7 Information without a court order, warrant, or subpoena. Upon information and
8 belief, the Money Transfer Defendants’ and Database Defendant’s data dragnet
9 operation gave unfettered access to Plaintiffs’ Protected Personal Information to
10 over 700 law enforcement entities.

11 9. Plaintiffs were unaware that their Protected Personal Information was
12 being shared with third parties TRAC and Forcepoint, who were not disclosed as
13 third parties that may have access to Plaintiffs’ Protected Personal Information.
14 Plaintiffs were likewise unaware that their Protected Personal Information was to be
15 indefinitely held in a data dragnet repository to be shared with further third parties,
16 including law enforcement agencies who were given access to the database without
17 warrant, subpoena, or court order. Plaintiffs did not consent to any such conduct.

18 10. Such an invasion of Plaintiffs’ privacy is anathema to California law,
19 policy, and equity.

20 11. Accordingly, Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, Bertha
21 Gonzalez Meza, Griselda Aviles Carrillo, and Jose Gerardo Vallejo Perez on behalf
22 of themselves and all others similarly situated, bring this suit for statutory penalties,
23 actual damages, and injunctive relief to avail Plaintiffs and Class members of their
24 constitutional and statutory privacy rights, make Plaintiffs and Class members
25 whole, and prevent this unconscionable conduct from ever occurring again.
26
27
28

I. PARTIES

12. Plaintiff Jose Guzman is a natural person domiciled in California. He resides in Chula Vista, California.

13. Plaintiff Fortino Rutilo Jimenez is a natural person domiciled in California. He resides in Montebello, California.

14. Plaintiff Bertha Gonzalez Meza is a natural person domiciled in California. She resides in Moreno Valley, California.

15. Plaintiff Griselda Aviles Carrillo is a natural person domiciled in California. She resides in Highland, California.

16. Plaintiff Jose Gerardo Vallejo Perez is a natural person domiciled in California. He resides in Los Angeles, California.

17. Defendant Western Union Financial Services, Inc. (“Western Union”) is a multinational financial services company incorporated in the State of Colorado. Its headquarters are in Denver, Colorado. Western Union offers and provides remittance transfers to consumers in 50 states, including California, and it regularly transacts and has transacted business in this district. Western Union Financial Services, Inc. is registered to do business in the state of California (2176772) with a CA Registered Corporate Agent located at 330 North Brand Blvd, Glendale, California.

18. Defendant MoneyGram Payment Systems, Inc. (“MoneyGram”) is a Delaware corporation in the money services business, offering international money transfers and bill pay. MoneyGram Payment Systems, Inc. is registered to do business in the state of California (19733691) with a CA Registered Corporate Agent located at 330 North Brand Blvd, Glendale, California. MoneyGram regularly transacts business in the state of California, including in this district.

19. Defendant Forcepoint LLC (“Forcepoint”) is a Delaware limited liability company with its headquarters and principal place of business in Austin,

1 Texas. Forcepoint is registered to do business in the state of California
2 (201607910169) with a CA Registered Corporate Agent located at 7801 Folsom
3 Boulevard #202, Sacramento, California. Forcepoint regularly transacts business in
4 California, including in this district.

5 20. Defendant Dolex Dollar Express Inc. (“Dolex”) is a Texas corporation.
6 Dolex is a multinational financial services company incorporated in the state of
7 Texas with its headquarters and principal place of business in Houston, Texas. Dolex
8 offers international remittances, money orders, payments, check cashing, and
9 installment loans. Dolex is registered to do business in the state of California
10 (2129392) with a CA Registered Corporate Agent located at 330 North Brand Blvd,
11 Glendale, California.

12 II. JURISDICTION AND VENUE

13 21. This Court has subject matter jurisdiction over Plaintiffs’ claims
14 pursuant to 28 U.S.C. § 1332. The Court also has subject matter jurisdiction pursuant
15 to 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds \$5 million,
16 there are over 100 members in the proposed Class, and at least one member of the
17 proposed Class is a citizen of a state or country different from at least one Defendant.

18 22. This Court has personal jurisdiction over the Defendants because each
19 regularly transacts business in and throughout this district, and the wrongful acts
20 alleged in this Complaint were committed within this district.

21 23. Venue is proper in this District under 28 U.S.C. § 1391(b) because a
22 substantial part of the events or omissions giving rise to Plaintiffs’ claims occurred
23 in and emanated from this district.

24 //

25 //

26 //

27 //

III. FACTUAL ALLEGATIONS

A. How Money Transfer Services and Transactions Work

24. Western Union was founded in 1851 as a company operating primarily in telegraph services, but eventually shifted its focus to cross-border money transfers, largely marketing its services to immigrants. Similarly, MoneyGram was formed to provide money transfer services to consumers globally.

25. Undeniably, this business model is based upon a booming market. Money transfers, or remittances as they are often called, are estimated to grow by 1.4% to \$656 billion in 2023, up from \$647 billion in 2022.⁴ The United States is one of the largest remitters and, notably, Mexico received the second highest level of remittances in 2022.

26. As providers of money transfer services, the Money Transfer Defendants' consumer base includes individuals spanning many countries and commonly without bank accounts. Without a bank account, many individuals cannot take advantage of electronic wire transfers or electronic checking to transfer money. Or as is sometimes the case, money transfer services through providers such as the Money Transfer Defendants are more cost-effective. To send money to a distant place, consumers can use a money transfer service, such as those offered by the Money Transfer Defendants to quickly send money abroad.

27. To earn a profit as a money transfer service, Money Transfer Defendants charge fees related to each transaction, as well as by setting exchange rates above market rate.

⁴ The World Bank, *Remittances Remain Resilient but Likely to Slow*, June 13, 2023, <https://www.worldbank.org/en/news/press-release/2023/06/13/remittances-remain-resilient-likely-to-slow> (last visited, February 12, 2024).

1 28. The money transfer process largely mirrors the following: (1) a sender
2 typically brings cash to a physical store where a representative of one of the Money
3 Transfer Defendants receives it and obtains information from the sender; (2) the
4 Money Transfer Defendants' representative also obtains information related to the
5 recipient of the money transfer and process the transaction; and (3) the recipient of
6 the transfer visits a physical location of the Money Transfer Defendants where the
7 money is delivered to them.

8 29. Consumers also transfer money using an online website or mobile
9 application that follows a similar process as outlined above but done through a
10 similar online or mobile process.

11 **B. Western Union Cooperates With Unlawful Data Dragnet**
12 **Operation**

13 30. In 2006, the Arizona Attorney General served administrative subpoenas
14 under Arizona Revised Statute § 12-2315 and § 6-1242 seeking bulk transaction
15 data related to money transfers conducted through Western Union by its consumers.
16 The facially improper subpoenas sought data relating to every send and each receive
17 transaction of \$300 and greater received in the state of Sonora, Mexico, on a weekly
18 basis as each week becomes available, beginning with January 1, 2004, and ending
19 with December 31, 2006. The subpoena sought 49 separate data fields worth of
20 information for every \$300 or greater transaction over this two-year period.

21 31. Western Union initially fought the enforcement of the subpoenas
22 against them, taking the enforceability question to the Arizona Court of Appeals.

23 32. A year later, in *State ex rel. Goddard v. Western Union Fin. Servs., Inc.*,
24 216 Ariz. 361 (App. 2007) the Arizona Court of Appeals held that the Attorney
25 General's subpoenas were unenforceable as a matter of law. The court found the
26 breadth of the subpoenas was impermissible and not reasonably articulated. In short,
27
28

1 the subpoenas violated the clear and well-defined principles of Fourth Amendment
2 particularity requirements, as well as similar requirements under Arizona law.

3 33. The Arizona Attorney General then sued Western Union under a state
4 anti-money laundering law.

5 34. To settle the anti-money laundering suit with the Arizona Attorney
6 General, in 2010 Western Union agreed to voluntarily produce, on an ongoing basis,
7 its consumers' personal identifying information (the "Western Union Settlement").

8 **1. Western Union Funds TRAC's Unlawful Data Dragnet**
9 **Operation**

10 35. In 2014, the Western Union Settlement was amended and expanded as
11 follows:

12 a. First, Western Union was required to deliver full transaction data
13 relating to all transactions sent to or from California, Arizona, New
14 Mexico, Texas, and the country of Mexico. Western Union was
15 required to continue sending this information over the next five years
16 until June 30, 2019.

17 b. Second, Western Union was required to pay hundreds of
18 thousands of dollars to establish and monetarily supplement the
19 Transaction Record Analysis Center, Inc. ("TRAC"), which would
20 house the data sent from Western Union. In fact, Western Union was
21 required to pay TRAC \$150,000 per month and also make a one-time
22 payment of \$250,000.00 to fund privacy, confidentiality, and
23 information security measures.

24 36. While early court records surrounding the Western Union Settlement
25 refer to TRAC as the "State Center," the incorporation, tax records, and funding by
26 Western Union state otherwise.

1 37. TRAC is not a governmental entity. Per its bylaws, TRAC was
2 incorporated in 2014 under the laws of Arizona as a non-profit corporation with the
3 purpose of promoting education, research, and training activities in the field of anti-
4 money laundering. Further, the bylaws hold that TRAC would receive funds and
5 research, train, and educate law enforcement agencies nationwide in the area of anti-
6 money laundering.

7 38. TRAC's tax filings confirm it is a 501(c)(3) non-profit, not a
8 government agency.

9 **2. TRAC Retains Forcepoint To Facilitate the Access,
10 Analysis, Exfiltration, and Disclosure of the Data Dragnet
11 Operation to Myriad Law Enforcement**

12 39. According to a 2015 TRAC Data Policy, TRAC provides analytical and
13 data-related assistance to “need-to-know investigators, analysts, and prosecutors in
14 their efforts to disrupt criminal organizations and dismantle their operations by
15 providing resources, expertise, meaningful data analysis, training, and
16 organizational collaboration.” Moreover, TRAC provides law enforcement with
17 analytical and technical training regarding access to and the use of the TRAC system.

18 40. As an entity, TRAC maintains an electronic database of all the
19 Protected Personal Information it receives from Money Transfer Defendants.

20 41. Once users receive training by TRAC, they have access to its database
21 and requisite software interface, reports, analytics, and Protected Personal
22 Information received from the Money Transfer Defendants.

23 42. To maintain, access, analyze, and use the database, TRAC contracted
24 with Forcepoint to provide, *inter alia*, “virtual data warehousing, federated search,
25
26
27
28

1 powerful algorithms for automated information discovery and intuitive workflow
2 tools.”⁵

3 43. Forcepoint’s tailored services would also allow “access to hundreds of
4 sources that an organization deems mission critical,” quick access to “understand,
5 analyze, react to, and share massive amounts of data,” and its services could “[s]peed
6 investigations with an easy-to-use information sharing and analysis platform proven
7 to enhance productivity and reduce crime.”⁶

8 44. With Forcepoint’s products/services, the TRAC database was now
9 accessible, searchable, and shareable by law enforcement officers, agents, or
10 investigators that received training from TRAC.

11 **C. HSI Joins TRAC and Forcepoint’s Unlawful Data Dragnet**
12 **Operation**

13 45. Once the Western Union Settlement ended in 2019, HSI began issuing
14 customs summons requesting Western Union transmit and disclose the Protected
15 Personal Information data of its consumers directly to TRAC.

16 46. Based upon its litigation against the Arizona Attorney General, Western
17 Union understood these types of data dragnet surveillance sweeps were facially
18 unlawful. The breadth of time range, number of data fields, and sheer number of
19 impacted consumers lacks articulation and specificity on its face. Indeed, the
20 Arizona Court of Appeals held as much.

21
22
23
24 ⁵ Forcepoint, “Connecting the Dots to Solve the Case: Forcepoint Data Analyzer
25 Capabilities”, [https://www.forcepoint.com/resources/webcasts/connecting-dots-
solve-case-forcepoint-data-analyzer-capabilities](https://www.forcepoint.com/resources/webcasts/connecting-dots-solve-case-forcepoint-data-analyzer-capabilities) (last visited April 2, 2024).

26 ⁶ Forcepoint, “Connecting the Dots to Solve the Case: Forcepoint Data Analyzer
27 Capabilities”, [https://www.forcepoint.com/resources/webcasts/connecting-dots-
solve-case-forcepoint-data-analyzer-capabilities](https://www.forcepoint.com/resources/webcasts/connecting-dots-solve-case-forcepoint-data-analyzer-capabilities) (last visited April 2, 2024).

1 47. Moreover, Western Union, as a sophisticated entity trading on the New
2 York Stock Exchange, knew or should have known the subpoenas from HSI were
3 patently violative of particularity requirements and unenforceable as a matter of law.

4 48. Nevertheless, Western Union voluntarily collected, compiled,
5 transmitted, and disclosed Plaintiffs' Protected Personal Information directly to
6 TRAC and/or Forcepoint in response to HSI's facially invalid customs summonses.

7 49. From 2019 to January 2022, HSI received 6,211,000 records from
8 Western Union and Maxi, another money transfer company.

9 50. In early 2022 after Senator Ron Wyden brought to light HSI's improper
10 use of customs summonses, HSI promptly withdrew them.

11 51. On information and belief, from 2019 to 2022 Western Union disclosed
12 Protected Personal Information of its consumers to the Database Defendant, with
13 categories similar to those requested from the Arizona Attorney General, including,
14 but not limited to, the following information for each send and receive transaction
15 over \$500 to or from California, Arizona, New Mexico, Texas, and the country of
16 Mexico:

17 a. (1) sender and receiver name, (2) sender and receiver address, (3)
18 sender and receiver city, (4) sender and receiver state, (5) sender and
19 receiver zip, (6) sender and receiver phone number, (7) sender and
20 receiver date of birth, (8) sender and receiver occupation, (9) sender
21 and receiver identification type, (10) sender and receiver identification
22 type description, (11) sender and receiver identification issuer, (12)
23 sender and receiver identification number, (13) sender and receiver
24 social security number;

25 b. For web-based transfers: (1) Sender Internet Protocol Address
26 used during web account creation, (2) Sender Internet Protocol Address
27 used to send transaction, (3) send email address used to create web
28

1 based account, (4) sender email address used to send transaction, (5)
2 sender source account number, (6) sender name on web based account,
3 (7) sender included reasons for transaction.

4 52. On information and belief, Western Union continues to improperly
5 disclose Plaintiffs' Protected Personal Information to the Database Defendant.

6 53. Therefore, the Database Defendant continues to have access to
7 Plaintiffs' Protected Personal Information, causing Plaintiffs' Protected Personal
8 Information to be subject to disclosure to each law enforcement agency, or any other
9 person or entity, with access to the TRAC/Forcepoint system.

10 54. In voluntarily transmitting, transferring, and disclosing Plaintiffs'
11 Protected Personal Information to the Database Defendant, Western Union failed to
12 implement, uphold, or maintain reasonable security procedures and practices
13 appropriate to the nature of Plaintiffs' Protected Personal Information.

14 55. At no point did Western Union disclose to Plaintiffs that it would
15 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information
16 based upon unlawful requests or facially invalid subpoenas or summonses. Nor did
17 Plaintiffs consent to any such conduct.

18 56. At no point did Western Union disclose to Plaintiffs that it would
19 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information to
20 a third-party non-profit named TRAC or Forcepoint. Nor did Plaintiffs consent to
21 any such conduct.

22 57. At no point did Western Union disclose to Plaintiffs that it had an
23 ongoing relationship with TRAC or Forcepoint, nor did Plaintiffs acknowledge or
24 consent to such relationship.

25 58. At no point did Western Union disclose to Plaintiffs that it would
26 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information to
27 undisclosed third parties or that the undisclosed third parties would permit an
28

1 additional subsequent disclosure to hundreds of law enforcement agencies without
2 any associated lawful request from such agencies. Nor did Plaintiffs consent to any
3 such conduct.

4 **D. MoneyGram and Dolex Join TRAC and Forcepoint's Unlawful**
5 **Data Dragnet Operation**

6 59. In 2019, while Western Union was turning over its own consumers
7 Protected Personal Information to the Database Defendant in conjunction with HSI
8 summonses, MoneyGram and Dolex were regularly sent subpoenas from the
9 Arizona Attorney General under Arizona Revised Statute § 13-2315 seeking a trove
10 of data related to each money transfer.

11 //

12 //

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //


24 //

25 //

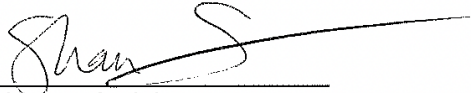
26 //

27 //

60. An exemplar MoneyGram subpoena below demonstrates the breadth of the information sought:

	STATE OF ARIZONA OFFICE OF ATTORNEY GENERAL
	2005 North Central Avenue Phoenix, Arizona 85004 (602) 542-8431
REQUEST TO PRODUCE RECORDS	
TO: MoneyGram Payment Systems Attn: Melissa Grant ref. Law Enforcement Subpoena Compliance 1550 Utica Avenue South, Ste. 100 Minneapolis, MN 55416-5312	
YOU ARE HEREBY COMMANDED, pursuant to A.R.S. § 13-2315, to produce for examination and copying by the Attorney General of the State of Arizona the following described records:	
Data, including the data fields described on the attached Data Appendix, relating to each send and each receive transaction of \$500 and greater, sent to or from the states of Arizona, California, New Mexico, Texas and to or from the country of Mexico, on a bi-weekly schedule as each such period becomes available, beginning with July 1, 2021 and ending with June 30, 2022. (PLEASE INCLUDE THE ADDITIONAL DATA FIELD FOR THE SUBPOENA IDENTIFICATION NUMBER. FOR THIS DATA FIELD PLEASE INCLUDE REFERENCE NUMBER: AZAG2021RTP2)	
The data is to be delivered electronically to the Arizona Attorney General's Office by delivery to its "SFTP" (Secure File Transfer Protocol) site in a delimited text files format.	

Please contact the Arizona Attorney General's Office through its investigator Chad Brink at chad.brink@azag.gov for any questions regarding production of this request and through its agent Mike Robinson at mike.robinson@forcepoint.com for the secure VPN address, and to define a new CSV standard if necessary, for the data delivery.


Shawn Steinberg
Assistant Attorney General
Arizona Attorney General's Office

61. Moreover, the above MoneyGram subpoena excerpts exemplify Forcepoint's initial role as the direct contact for "data delivery" of Plaintiffs' Protected Personal Information.⁷ In contrast to Forcepoint's case study (Exhibit B)⁸ and datasheet discussed below (Exhibit C),⁹ the excerpted subpoena shows Forcepoint's direct relationship with the Protected Personal Information for secure VPN address to, presumably, upload and deliver the incoming Protected Personal Information.

62. The Arizona Attorney General continued to send these administrative subpoenas to various money transfer entities from 2019 through at least 2022.

63. Notably, as shown above, these subpoenas from the Arizona Attorney General required MoneyGram to remit the requested Protected Personal Information directly to Forcepoint (TRAC's vendor), not the Arizona Attorney General.

64. From 2019 through 2022, MoneyGram and Dolex received these subpoenas requesting bulk transaction data for all transactions \$500 or greater that they serviced between California, Arizona, New Mexico, Texas, and the country of Mexico for 6–12 month periods, to be renewed with forthcoming subpoenas.

65. The subpoenas sought the following information:

- a. (1) sender and receiver name, (2) sender and receiver address, (3) sender and receiver city, (4) sender and receiver state, (5) sender and receiver zip, (6) sender and receiver phone number, (7) sender and receiver date of birth, (8) sender and receiver occupation, (9) sender and receiver identification type, (10) sender and receiver identification

⁷ Exhibit A, MoneyGram Subpoena, signed June 11, 2021, highlighting Forcepoint's complicity in the initial data delivery and unlawful data dragnet directly seeking Plaintiffs' Protected Personal Information.

⁸ See Exhibit B, Forcepoint, *Case Study – Arizona Financial Crimes Task Force*.

⁹ See Exhibit C, Forcepoint Datasheet, *Forcepoint SureView Analytics Big Button for Law Enforcement Solution*, at p.4.

1 type description, (11) sender and receiver identification issuer, (12)
2 sender and receiver identification number, (13) sender and receiver
3 social security number;

4 b. For web-based transfers: (1) Sender Internet Protocol Address
5 used during web account creation, (2) Sender Internet Protocol Address
6 used to send transaction, (3) send email address used to create web
7 based account, (4) sender email address used to send transaction, (5)
8 sender source account number, (6) sender name on web based account,
9 (7) sender included reasons for transaction.

10 66. To be clear, the Protected Personal Information was not sent by
11 MoneyGram or Dolex to law enforcement. Instead, it was sent to a non-
12 governmental entity TRAC via Forcepoint.

13 67. Neither TRAC nor Forcepoint are government entities.

14 68. As sophisticated entities, MoneyGram and Dolex knew or should have
15 known that the Arizona Attorney General's subpoenas were patently and facially
16 unenforceable as demonstrated by the prior Arizona Court of Appeals opinion on
17 virtually identical facts.

18 69. Nevertheless, MoneyGram and Dolex disclosed the requested Protected
19 Personal Information to the Database Defendant, from 2019 through at least 2022.

20 70. On information and belief, MoneyGram and Dolex continue to disclose
21 Plaintiffs' Protected Personal Information to the Database Defendant. Accordingly,
22 the Database Defendant continues to have access to Plaintiffs' Protected Personal
23 Information.

24 71. Because the Database Defendant has access to Plaintiffs' Protected
25 Personal Information, Plaintiffs' Protected Personal Information is subject to
26 subsequent disclosure to each law enforcement agency, or other person, with access
27 to the TRAC/Forcepoint system.

1 72. In voluntarily collecting, compiling, transmitting, and disclosing
2 Plaintiffs' Protected Personal Information, MoneyGram and Dolex failed to
3 implement, uphold, or maintain reasonable security procedures and practices
4 appropriate to the nature of Plaintiffs' Protected Personal Information.

5 73. At no point did MoneyGram or Dolex disclose to Plaintiffs that they
6 would collect, compile, transmit, or disclose Plaintiffs' Protected Personal
7 Information based upon unlawful requests or facially invalid subpoenas or
8 summonses. Nor did Plaintiffs consent to any such conduct.

9 74. At no point did MoneyGram or Dolex disclose to Plaintiffs that they
10 would collect, compile, transmit, or disclose Plaintiffs' Protected Personal
11 Information to a third-party non-profit named TRAC or Forcepoint. Nor did
12 Plaintiffs consent to any such conduct.

13 75. At no point did MoneyGram or Dolex disclose to Plaintiffs that they
14 had an ongoing relationship with TRAC or Forcepoint, nor did Plaintiffs
15 acknowledge or consent to such relationship.

16 76. At no point did MoneyGram or Dolex disclose to Plaintiffs that they
17 would collect, compile, transmit, or disclose Plaintiffs' Protected Personal
18 Information to undisclosed third parties or that the undisclosed third parties would
19 permit an additional subsequent disclosure to hundreds of law enforcement agencies
20 without any associated lawful request from such agencies. Nor did Plaintiffs consent
21 to any such conduct.

22 **E. Forcepoint's Services and/or Products Create Secondary**
23 **Exfiltration, Access, Observation, Analysis, and Disclosure of**
24 **Troves of Protected Personal Information to Myriad Law**
25 **Enforcement**

26 77. After the Money Transfer Defendants transmitted, disclosed, or
27 otherwise sent the Protected Personal Information to TRAC/Forcepoint,
28

Forcepoint's products/services allowed for the data to be accessed, searched, analyzed, observed, viewed, or otherwise disclosure of the Protected Personal Information to be received by law enforcement, as explained in the proceeding subsections.

1. Forcepoint's Case Study

78. Forcepoint publicly released a case study that expressly describes the capabilities and role of its services and/or products in this unlawful data dragnet seeking Plaintiffs' Protected Personal Information, a true and accurate copy of which is attached as Exhibit B.¹⁰

79. First, the case study defines Forcepoint's "Customer" as the Arizona Financial Crimes Task Force (AZFCTF), the "Platform" as Transaction Record Analysis Center (TRAC), and "User Base" as "International, predominately USA with concentration in the Southwest Border States."¹¹

80. The Forcepoint case study explains:

In January of 2014, the [Arizona Financial Crimes Task Force] (AZFCTF) funded the creation of the Transaction Record Analysis Center (TRAC), a centralized searchable database of the financial transactions of global money services business (MSBs). TRAC now serves as the intelligence component for AZFCTF and is staffed by analyst and law enforcement professionals recognized as experts in money laundering activity. The TRAC provides data, meaningful data analysis, collaboration and training to investigators, analysts and prosecutors nationwide in their efforts to disrupt criminal organizations and dismantle their operations.¹²

¹⁰ Exhibit B, Forcepoint, *Case Study – Arizona Financial Crimes Task Force*.

¹¹ *Id.*

¹² *Id.*

81. As noted in Forcepoint’s case study, TRAC serves as the intelligence component for AZFCTF, primarily focusing on the Southwest Border region of the United States, including and/or targeting California.¹³

82. Because the volume of data was so voluminous, a “simple query involving multiple names, addresses or telephone numbers, for example, took hours or days to complete,” Forcepoint provided its specifically tailored “analytical solution” entitled Forcepoint’s SureView Analytics and explained:

AZFCTF needed a solution that could manage the huge volumes of data flowing into the TRAC, as well as deliver an easy-to-use analytical platform to law enforcement and regulatory users. Today, Forcepoint’s SureView Analytics is providing AZFCTF with a turnkey analytical solution that is customized for the varied user community consisting of federal agents, analysts, state and local detectives as well as money services business regulators. **For each of these stakeholders, SureView Analytics delivers complete management of the environment from data ingestion to delivery of actionable analytics.** The TRAC portal offers a dashboard of easy to use analysis tools, training webinars and auditing functions. Through a secure private cloud, the solution avoids overhead expenses of onsite hosting, and offers scalability as needed. Queries can be returned in a matter of seconds instead of hours which turns the increasing volume of data transactions from an enemy into an ally.¹⁴

83. The Forcepoint case study makes explicit that Forcepoint provided “complete management of the environment from data ingestion to delivery of actionable analytics” with the result leading to myriad law enforcement access to access, search, view, observe, review, and consider the “actionable analytics” related to Protected Personal Information.¹⁵

¹³ *Id.*

¹⁴ *Id.* at 2 (emphasis added).

¹⁵ *Id.*

1 84. Forcepoint’s case study openly acknowledges the unlawful purpose
2 was to provide law enforcement agencies with access to a database that “**contains**
3 **more relevant data than what would be obtained in a traditional subpoena**
4 **process**” and that this “**data access** enables investigators to geospatially visualize
5 **criminal corridors of illegal transactions, saving thousands of man hours and**
6 **lengthy delays in the subpoena process.”¹⁶**

7 85. Forcepoint thus advertises its direct affront to due process and
8 constitutional protections of potentially millions of innocent civilians while
9 displaying how the underlying Protected Personal Information is “accessed” and
10 ultimately used—regardless of “ownership” of the data.

11 //

12 //

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

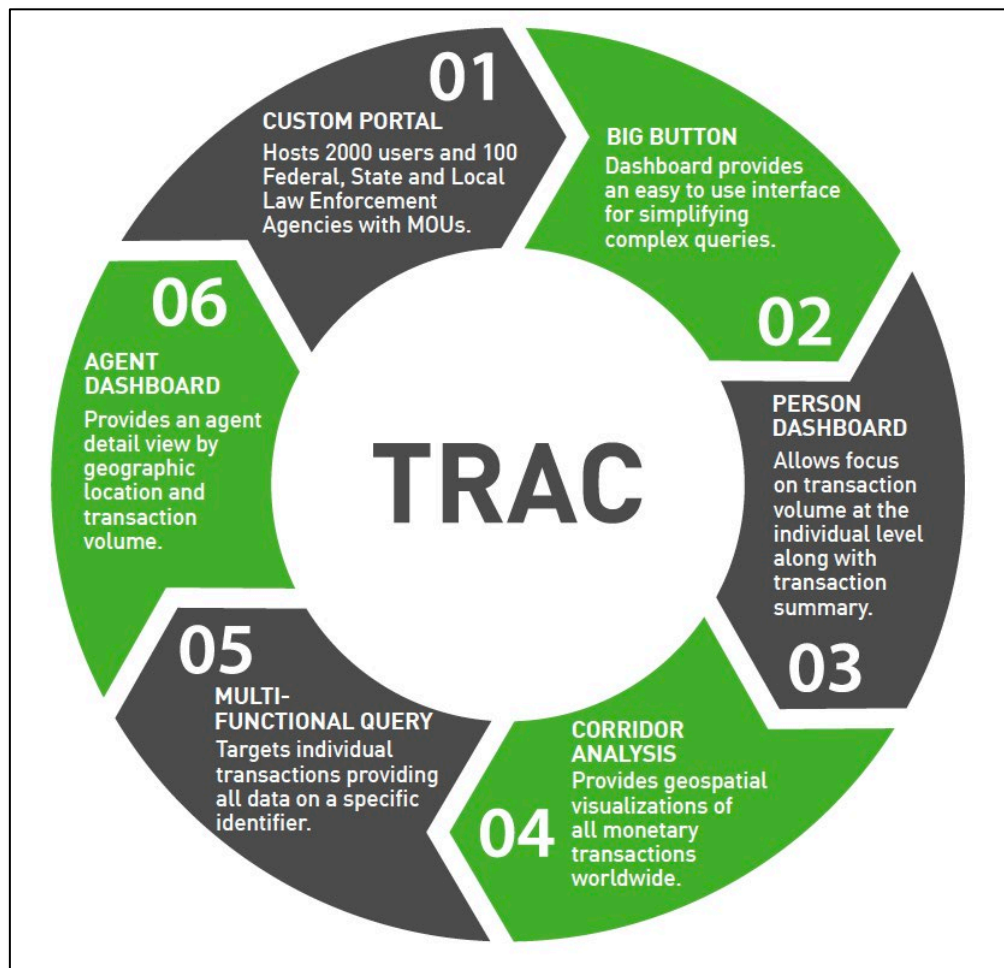
23 //

24 //

25 //

26
27 ¹⁶ *Id.* (emphasis added).

86. Lastly, the case study indicates the ease of its use paired with its extensive data analytics and sharing capabilities, as shown in the graphic below. Notably, Forcepoint discusses its “Big Button” dashboard that “provides an easy-to-use interface for simplifying complex queries.” And the depth of Protected Personal Information viewing is also explained: “Person Dashboard Allows focus on transaction volume at the individual level along with transaction summary.”¹⁷



¹⁷ *Id.* (emphasis added).

2. Forcepoint's Datasheet: Forcepoint SureView Analytics Big Button for Law Enforcement Solution Amounts to a Data Subterfuge

87. Forcepoint created a SureView Analytics datasheet disclosure called “Big Button for Law Enforcement Solution,” a true and accurate copy of which is attached as Exhibit C.¹⁸

88. The datasheet makes clear the “solutions” Forcepoint offers, such as Big Button, are a means to maintain “ownership” of the data with the original source and “comply” with law enforcement Freedom of Information Act requirements, by creating a system that is “outside” the ordinary FOIA disclosure process.¹⁹

89. Forcepoint's SureView Analytics Big Button, as discussed in the case study, is:

[A]n agile, adaptable, and scalable federated search and visualization platform that boosts the speed, collaboration and efficacy of investigative and analytical divisions. It provides **access to hundreds of sources** that an organization deems mission critical and applies automation, **advanced data discovery**, and visualization capabilities to rapidly deliver key insight to investigations. As individuals set and receive alerts to and from their **mobile devices**, they are empowered to immediately continue an investigation **regardless of their physical location**.²⁰

90. SureView Analytics Big Button is so easy, it can be used from a law enforcement officers cellphone, from anywhere: “Time-consuming and extensive search algorithms hide behind the friendly facade of a simple round button, bringing the capability of an advanced analyst to the fingertips of an entry level workforce.”²¹

¹⁸ Exhibit C, Forcepoint Datasheet, *Forcepoint SureView Analytics Big Button for Law Enforcement Solution*.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

91. The datasheet explains how Forcepoint’s SureView analytics permits linking of various datasets and federated searching with “**instant access to all data necessary**” to create the “**ultimate virtual data warehouse**”²²:

Link Analysis

With link analysis visualizations of a search query on your mobile device, investigators can quickly deduce and act on next steps of a situation. Automated data discovery technology quickly unearths relationships between information stored across hundreds of data sources and returns information as actionable intelligence because it visualizes the associations between individuals, events, activities, locations, etc., enabling the investigator to naturally deduce progression of next steps of an investigation.

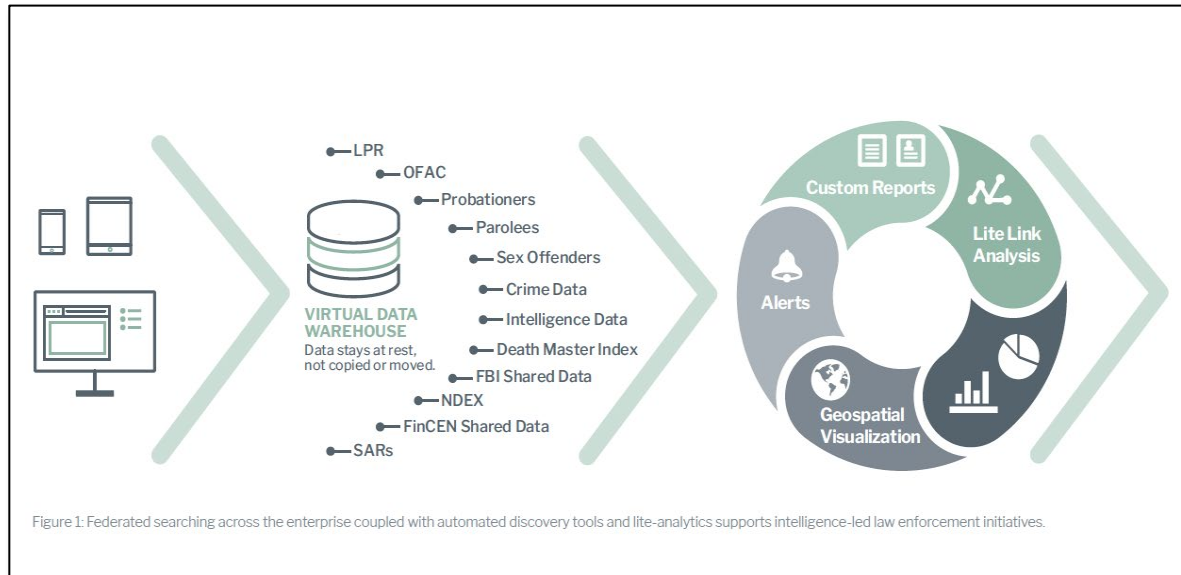
Federated Searching

Federated searching ensures that investigators and analysts have instant access to all data necessary to develop an inclusive picture of a situation. It seamlessly connects any number of local and remote data sources to create the ultimate virtual data warehouse that eliminates data duplication and enables effective information sharing. The timely process of cross jurisdictional and third-party approvals for access to information from multiple agencies is overcome.

92. As shown below in figure excerpts, Forcepoint’s datasheet exemplifies how its services allow data to “stay at rest, not copied or moved,” yet

²² *Id.*

can still be accessed, observed, or otherwise used to create reports, analysis, alerts, and/or visualizations.²³



93. SureView Analytics is touted as being able to “analyze and pull data from data lakes and unlike other case management tools, **ownership of data remains at the source.**”²⁴ Likewise, Forcepoint acknowledges that transferring ownership can create problems: “Ownership of the data stays with original source. Unlike other technology options, the data is not ingested into a proprietary database therefore ownership of the data stays with the data owner, reducing the need to share ownership of the data with a third-party source which can create problems for the unit in the long run.”²⁵

94. Forcepoint seemingly indicates that because the data is only “accessed,” ownership does not transfer, illustrated by the separation of the Virtual Data Warehouse from any direct lines to the potential accessing parties as shown in the figure above.

²³ *Id.* at 2.

²⁴ *Id.*

²⁵ *Id.*

1 95. Forcepoint even acknowledges the potential illegality of “moving
2 data”:²⁶

3
4 Often moving data from its
5 original source can compromise
6 the validity of the data and
7 in some cases is illegal. With
8 SureView federated search,
9 analysts can query and view
10 data from multi jurisdictions
11 and multiple databases without
12 moving it. The ability to view data
13 at its source also eliminates the
14 need for onsite storage.
15
16

17 96. This is further exemplified by Forcepoint’s own statements directed
18 toward law enforcement, stating “[c]omply with Law Enforcement Freedom of
19 Information Act (FOIA) requirements by leaving ownership of the data at the
20 original source. Unlike other technologies that ingest data, **SureView Analytics**
21 **relieves the unit from legal responsibility of reporting on the data due to**
22 **ingestion.**”²⁷ Thus, Forcepoint directly posits that law enforcement can access the
23 underlying data and gain from it the needed information—what the data tells and
24

25 ²⁶ Exhibit C, Forcepoint Datasheet, *Forcepoint SureView Analytics Big Button for*
26 *Law Enforcement Solution*.

27 ²⁷ Exhibit C, Forcepoint Datasheet, *Forcepoint SureView Analytics Big Button for*
28 *Law Enforcement Solution* (emphasis added).

1 indicates—all while “avoiding” obligations to comply with the law by not
2 “ingesting” the same data or information.

3 97. As a solution or workaround to potential illegalities of “moving data,”
4 Forcepoint posits what its services can do: “[t]he technology mimics the outcome of
5 a traditional warehouse while preserving the custody, security and physical
6 ownership of the data on the original source (never copied or moved).”²⁸

7 98. By Forcepoint’s own analogy, Forcepoint acts as the keyholder to the
8 original “owner’s” warehouse and duly decides who may get the “key” to the
9 warehouse to simply “see” or “access” the contents of the warehouse therein, but
10 without removing anything from the warehouse—only accessing, searching,
11 viewing, observing.²⁹

12 99. That is, Forcepoint’s SureView Analytics controls and specifically
13 allows the access, searching, viewing, observing, analysis/analytics, and otherwise
14 disclosure of the underlying data, regardless of who “owns” or holds it. And
15 Forcepoint provides “actionable analytics” to ensure that third party searching the
16 entire warehouse is easy as can be—from hours to seconds.³⁰

17 100. Nevertheless, Forcepoint allows instantaneous “searching of live
18 data.”³¹

24 ²⁸ *Id.* at 4.

25 ²⁹ *Id.*

26 ³⁰ See Exhibit B, Forcepoint, *Case Study – Arizona Financial Crimes Task Force.*

27 ³¹ Exhibit C, Forcepoint Datasheet, *Forcepoint SureView Analytics Big Button for*
28 *Law Enforcement Solution*, at p.4.

▶ **Instantaneously search live data** across internal or external databases, websites, emails or office documents.

Latency impacts are greatly reduced because unlike other case management tools that download and store data, SureView Analytics accesses live data. If data is unavailable, analysts receive notice but are able to work with the previous data set until the new data is available.

101. Forcepoint’s business model is clear from its case study and datasheet disclosures—provide and share information gleaned from the data, but not the physical hosting or physical transfer of the actual underlying data. Extract what is needed—the information—and avoid “legal obligations” by not “ingesting” the data.³²

102. By design, the TRAC/Forcepoint system allows myriad law enforcement to access, search, review, observe, and/or analyze Personal Protected Information in a circumvention of due process by collecting, gathering, obtaining, receiving (whether actively or passively), accessing, compiling, holding, and/or storing the Protected Personal Information of Plaintiffs and other innocent civilians to then provide visibility, observation, access, and analysis related to monetary transaction data worldwide, all while never changing “ownership” of the underlying data. This is all done surreptitiously, without Plaintiffs’ knowledge or consent.

³² See Exhibits B–C.

3. Forcepoint Allows and Controls Unlawful Access to Plaintiffs' Protected Personal Information.

103. As indicated in Forcepoint's case study³³ and datasheet,³⁴ Plaintiffs' Protected Personal Information is subject to unlawful access by myriad law enforcement by and through the conduct, actions, products, and/or services of Forcepoint.

104. Forcepoint's SureView Analytics permits law enforcement to unlawfully access, search, view, observe, receive analytics, and otherwise receive the disclosure of the Protected Personal Information contained within TRAC.³⁵

105. On information and belief, Forcepoint's SureView Analytics "Big Button" grants access to the underlying information from TRAC to law enforcement mobile devices.³⁶

106. As reflected in a May 2, 2022, internal TRAC email from the TRAC Executive Director, Rich Lebel, to Carol Keppler entitled "TRAC Docs," the TRAC/Forcepoint database was accessible by over 700 law enforcement agencies.³⁷

107. These include various California agencies, departments, or groups such as:³⁸

- a. Bakersfield California Police Department
- b. California Central Valley HIDTA (High Intensity Drug Trafficking Area)
- c. California Department of Consumer Affairs Division

³³ Exhibit B.

³⁴ Exhibit C.

³⁵ Exhibit B, at p.2 ("The TRAC, supported by Forcepoint's SureView Analytics solution provides agencies with the fast data analysis they need.")

³⁶ Exhibit C, Forcepoint Datasheet, *Forcepoint SureView Analytics Big Button for Law Enforcement Solution*, at p.1.

³⁷ Exhibit D, List of Agencies with Access to TRAC and Accompanying Email.

³⁸ *Id.*

- d. California Department of Corrections and Rehabilitation
- e. California Department of Fish and Wildlife
- f. California Department of Health Care Services
- g. California DOJ/Attorney General
- h. California Office of Correctional Safety
- i. California State Prison OIA
- j. California Sub Abuse and State Prison
- k. CBP-San Diego Field Office
- l. City of Santa Clara Police Department - California
- m. DEA Los Angeles Field Division
- n. DEA San Diego Field Division
- o. DEA San Francisco Field Division
- p. Escondido California Police Department
- q. Fairfield California Police Department
- r. Fremont California Police Department
- s. Glendale Police Department – California
- t. Glendora California Police Department
- u. LA County Sheriff’s Office
- v. Los Angeles Police Department
- w. Riverside County California Sherriff’s Department
- x. Ventura California Police Department
- y. Ventura County Sherriff’s Office California

108. Notably, TRAC identifies Forcepoint as an entity with access to the database.³⁹

³⁹ *Id.* at p. 12.

1 109. On information and belief, but for Forcepoint's SureView Analytics,
2 each of the preceding Californian individuals, entities, departments, agencies, or
3 groups (among any others) had or have full ability to access, search, view, observe,
4 receive analytics, and otherwise receive the disclosure of Plaintiffs' Protected
5 Personal Information that would not have been otherwise possible but for
6 Forcepoint.

7 **IV. TOLLING OF STATUTE OF LIMITATIONS**

8 110. Plaintiffs and the other members of the Class had neither actual nor
9 constructive knowledge of the facts constituting their claim for relief. They did not
10 discover, nor could they have discovered through the exercise of reasonable
11 diligence, the existence of Money Transfer Defendants' and Database Defendant's
12 conduct until shortly before filing this Complaint.

13 111. The Money Transfer Defendants and Database Defendant failed to
14 reveal facts sufficient to put Plaintiffs and the other Class members on notice. Money
15 Transfer Defendants and Database Defendant did not and do not inform their
16 consumers that their consumers' Protected Personal Information would be sent to
17 TRAC or Forcepoint, nor that subsequent parties would have access to such
18 Protected Personal Information. Rather, Defendants give consumers false and
19 misleading impressions of security, safety, and privacy as mentioned in their
20 marketing.

21 112. At no point did Money Transfer Defendants or the Database Defendant
22 disclose to Plaintiffs that each would collect, compile, transmit, or disclose
23 Plaintiffs' Protected Personal Information as alleged herein. Nor did Plaintiffs
24 consent to any such conduct.

25 113. Moreover, an ordinary person acting reasonably diligent would not
26 have had the time, resources, or specialized training to uncover the misconduct that
27 Money Transfer Defendants or the Database Defendant engaged in here.

1 114. Indeed, Plaintiffs exercised reasonable diligence to protect their
2 Protected Personal Information from interception, exfiltration, or disclosure. To be
3 sure, that is precisely why Plaintiffs used Money Transfer Defendants' services—
4 fast, safe, and (allegedly) secure means of transmitting money to consumers abroad.

5 115. Due to the Money Transfer Defendants' and the Database Defendant's
6 fraudulent concealment of their wrongful conduct, the running of the statute of
7 limitations has been tolled and suspended with respect to the claims and rights of
8 action of Plaintiffs and the other Class members as a result of such conduct.

9 **V. FACTS SPECIFIC TO PLAINTIFFS**

10 116. Plaintiff Jose Guzman ("Guzman") regularly used Western Union to
11 send money from California to Mexico in 2020, including in excess of \$500.
12 Guzman was never informed his Protected Personal Information would be disclosed
13 upon an unlawful request nor that Guzman's Protected Personal Information would
14 be disclosed to an unidentified third party named TRAC or Forcepoint. Guzman was
15 never informed his Protected Personal Information would remain in a mass database
16 accessible by hundreds of government agencies or others. Guzman never consented
17 to any such disclosure of his Protected Personal Information. If Guzman had known
18 about this invasion of his privacy, he would not have paid Western Union to process
19 the transaction, and would instead have searched for alternative options for sending
20 his money. Guzman is disturbed that his Protected Personal Information, along with
21 information about friends abroad, was disclosed to the Database Defendant and
22 ultimately hundreds of law enforcement agencies without his knowledge. Guzman
23 seeks the full statutory and actual damages allowable under law.

24 117. Plaintiff Bertha Meza ("Meza") regularly used Western Union to send
25 money from California to Mexico in 2022, including in excess of \$500. Meza was
26 never informed her Protected Personal Information would be disclosed upon an
27 unlawful request nor that Meza's Protected Personal Information would be disclosed
28

1 to an unidentified third party named TRAC or Forcepoint. Meza was never informed
2 her Protected Personal Information would remain in a mass database accessible by
3 hundreds of government agencies or others. Meza never consented to any such
4 disclosure of her Protected Personal Information. If Meza had known about this
5 invasion of her privacy, she would not have paid Western Union to process the
6 transaction, and would instead have searched for alternative options for sending her
7 money. Meza is disturbed that her Protected Personal Information, was disclosed to
8 the Database Defendant and ultimately, hundreds of law enforcement agencies
9 without her knowledge. Meza seeks the full statutory and actual damages allowable
10 under law.

11 118. Plaintiff Fortino Rutilo Jimenez (“Jimenez”) regularly used
12 MoneyGram to send money from California to Mexico in 2022, including in excess
13 of \$500. Jimenez was never informed his Protected Personal Information would be
14 disclosed upon an unlawful request nor that Jimenez’s Protected Personal
15 Information would be disclosed to an unidentified third party named TRAC or
16 Forcepoint. Jimenez was never informed his Protected Personal Information would
17 remain in a mass database accessible by hundreds of government agencies or others.
18 Jimenez never consented to any such disclosure of his Protected Personal
19 Information. If Jimenez had known about this invasion of his privacy, he would not
20 have paid MoneyGram to process the transaction, and would instead have searched
21 for alternative options for sending his money. Jimenez is disturbed that his Protected
22 Personal Information was disclosed to the Database Defendant and ultimately,
23 hundreds of law enforcement agencies without his knowledge. Jimenez seeks the
24 full statutory and actual damages allowable under law.

25 119. Plaintiff Griselda Aviles Carrillo “Carrillo” regularly used Dolex to
26 send money from California to Mexico in 2022, including in excess of \$500. Carrillo
27 was never informed her Protected Personal Information would be disclosed upon an
28

1 unlawful request nor that Carrillo's Protected Personal Information would be
2 disclosed to an unidentified third party named TRAC or Forcepoint. Carrillo was
3 never informed her Protected Personal Information would remain in a mass database
4 accessible by hundreds of government agencies or others. Carrillo never consented
5 to any such disclosure of her Protected Personal Information. If Carrillo had known
6 about this invasion of her privacy, she would not have paid Dolex to process the
7 transaction, and would instead have searched for alternative options for sending her
8 money. Carrillo is disturbed that her Protected Personal Information was disclosed
9 to the Database Defendant and ultimately, hundreds of law enforcement agencies
10 without her knowledge. Carrillo seeks the full statutory and actual damages
11 allowable under law.

12 120. Plaintiff Jose Gerardo Vallejo Perez ("Perez") regularly used Dolex to
13 send money from California to Mexico in 2020 and 2022, including in excess of
14 \$500. Perez was never informed his Protected Personal Information would be
15 disclosed upon an unlawful request nor that Perez's Protected Personal Information
16 would be disclosed to an unidentified third party named TRAC or Forcepoint. Perez
17 was never informed his Protected Personal Information would remain in a mass
18 database accessible by hundreds of government agencies or others. Perez never
19 consented to any such disclosure of his Protected Personal Information. If Perez had
20 known about this invasion of his privacy, he would not have paid Dolex to process
21 the transaction, and would instead have searched for alternative options for sending
22 his money. Perez is disturbed that his Protected Personal Information was disclosed
23 to the Database Defendant and ultimately, hundreds of law enforcement agencies
24 without his knowledge. Perez seeks the full statutory and actual damages allowable
25 under law.

VI. CLASS ACTION ALLEGATIONS

121. **Class and Subclass Definitions:** Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of themselves and a Class and Subclass of similarly situated individuals, defined as follows:

All California residents who used the services of any Money Transfer Defendant or Money Transfer Defendants' subsidiaries or affiliates and such residents' Protected Personal Information was sent to TRAC and/or Forcepoint ("the Class").

All California residents whose Protected Personal Information was sent to TRAC and/or Forcepoint and subsequently viewed, observed, analyzed, accessed, or disclosed. ("Database Defendant subclass").

The following people are also excluded from the Class and Subclass: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Money Transfer Defendants and Database Defendant, as well as Money Transfer Defendants' and Database Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Money Transfer Defendants or Database Defendant or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

122. **Numerosity:** On information and belief, the proposed Class includes hundreds of thousands, if not millions, of people. Members of the Class can be identified through Money Transfer Defendants' and Database Defendant's records.

123. **Commonality and Predominance:** There are many questions of law and fact common to Plaintiffs' and each Class members' claims, and those questions predominate over any questions that may affect individual class members. Common questions include but are not limited to the following:

- a. Whether Plaintiffs and the Class members are “consumers” under the California Consumer Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq.;
- b. Whether Money Transfer Defendants and Database Defendant are “businesses” under the California Consumer Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq.;
- c. Whether the Money Transfer Defendants and Database Defendant violated § 1798.150 of the California Consumer Privacy Rights Act;
- d. Whether the Money Transfer Defendants and Database Defendant violated Plaintiffs’ and Class members’ privacy rights in violation of the California Constitution;
- e. Whether Plaintiffs and members of the Class are entitled to injunctive relief, statutory damages, actual damages, and reasonable costs and attorney’s fees from Money Transfer Defendants and Database Defendant;
- f. Whether Money Transfer Defendants and Database Defendant should be enjoined from engaging in such conduct in the future; and
- g. The extent and form of any preliminary or equitable relief that the Court determines appropriate.

124. **Typicality:** Plaintiffs’ claims are typical of the claims of other members of the Class and Subclass in that Plaintiffs and the members of the Class and Subclass were harmed, continue to be harmed, and Money Transfer Defendants’ and the Database Defendant’s conduct gave rise to the claims of Plaintiffs, the Class, and the Subclass.

1 **125. Adequate Representation:** Consistent with Rule 23(a)(4), Plaintiffs
2 are adequate representatives of the Class because Plaintiffs are members of the Class
3 and committed to pursuing this matter against Money Transfer Defendants and the
4 Database Defendant to obtain relief for the Class. Plaintiffs have no conflicts of
5 interest with the Class. Plaintiffs' counsel are competent and experienced in
6 litigating class actions, including extensive experience in litigating consumer claims.
7 Plaintiffs intend to vigorously prosecute this case and will fairly and adequately
8 protect the interests of the Class.

9 **126. Policies Generally Applicable to the Class:** This class action is
10 appropriate for certification because Defendants have acted on grounds generally
11 applicable to the Class as a whole, thereby requiring the Court's imposition of
12 uniform relief to ensure compatible standards of conduct toward the members of the
13 Class and making final injunctive relief appropriate with respect to the Class as a
14 whole. The policies that Plaintiffs challenge apply to and affect members of the Class
15 uniformly, and Plaintiffs' challenge of these policies hinges on Money Transfer
16 Defendants' and the Database Defendant's conduct with respect to the Class and
17 Subclass as a whole, not on facts or law applicable only to Plaintiffs. The factual and
18 legal bases of Money Transfer Defendants and Database Defendant liability to
19 Plaintiffs and to the other members of the Class and Subclass are the same.

20 **127. Predominance and Superiority:** Consistent with Rule 23(b)(3) the
21 questions of law or fact common to class members predominate over any questions
22 affecting only individual members, a class action is superior to any other available
23 means for the fair and efficient adjudication of this controversy, and no unusual
24 difficulties are likely to be encountered in the management of this class action. The
25 purpose of the class action mechanism is to permit litigation against wrongdoers
26 even when damages to individual plaintiffs and class members may not be sufficient
27 to justify individual litigation. Here, the damages suffered by Plaintiffs, the Class,
28

1 and Subclass members are relatively small compared to the burden and expense
2 required to individually litigate their claims against Money Transfer Defendants and
3 the Database Defendant, and thus, individual litigation to redress Money Transfer
4 Defendants' and the Database Defendant's wrongful conduct would be
5 impracticable. Individual litigation by each Class member and Subclass member
6 would also strain the court system. Moreover, individual litigation creates the
7 potential for inconsistent or contradictory judgments and increases the delay and
8 expense to all parties and the court system. By contrast, the class action device
9 presents far fewer management difficulties and provides the benefits of a single
10 adjudication, economies of scale, and comprehensive supervision by a single court.

11 **128. Injunctive and/or Declaratory Relief. Fed. R. Civ. P. 23(b)(2).**
12 Money Transfer Defendants and the Database Defendant through their uniform
13 conduct, acted or refused to act on grounds generally applicable to the Class as a
14 whole, making injunctive and/or declaratory relief appropriate.

15 **129.** Plaintiffs anticipate the issuance of notice, setting forth the subject and
16 nature of the instant action, to the proposed Class members. Upon information and
17 belief, Defendants' own business records, other available records, and/or electronic
18 media can be utilized for the contemplated notices. To the extent that any further
19 notices may be required, Plaintiffs anticipate the use of additional media and/or
20 mailings.

21 **130.** Plaintiffs reserve the right to revise each of the foregoing allegations
22 based on facts learned through additional investigation and in discovery.

VII. CAUSES OF ACTION

COUNT 1

**Violation of the California Consumer Privacy Rights Act § 1798.150 et seq.
(On behalf of Plaintiffs, the Class, and Subclass against All Defendants)**

131. Plaintiffs and Class members incorporate the foregoing paragraphs as if set forth fully herein.

132. Plaintiffs bring this count on behalf of themselves and the Class.

133. The California Consumer Privacy Rights Act, § 1798.100, et seq. (“CCPA”) is a comprehensive statutory scheme that is to be liberally construed to empower and entitle Californians to know what personal information is collected about them and whether their personal information is sold or disclosed and to whom.

134. Plaintiffs are “consumers” as defined by the CCPA.

135. The Money Transfer Defendants and the Database Defendant are “businesses” as defined by the CCPA and therefore subject to liability thereunder.

136. The Money Transfer Defendants and the Database Defendant collected, gathered, obtained, received (whether actively or passively), accessed, compiled, held, and/or stored Plaintiffs’ Protected Personal Information as defined in Cal. Civ. Code § 1798.81.5(d)(1)(A), including but not limited to Plaintiffs’ first and last names, government identification, account numbers, and/or credit or debit card numbers.

137. Plaintiffs’ Protected Personal Information was voluntarily collected, accessed, stored, transmitted, and/or disclosed by Money Transfer Defendants and the Database Defendant in a nonencrypted and nonredacted form, or in some other form that permitted unauthorized individuals to access that information in violation of the CCPA.

138. Through this voluntary disclosure, Money Transfer Defendants and the Database Defendant breached their duty to implement, uphold, or maintain

1 reasonable security procedures and practices appropriate to the nature of Plaintiffs’
2 Protected Personal Information.

3 139. As a direct and proximate result of Money Transfer Defendants’ and
4 the Database Defendant’s failure to implement, uphold, or maintain reasonable
5 security procedures and practices appropriate to the nature of Plaintiffs’ Protected
6 Personal Information, Plaintiffs suffered unauthorized access, exfiltration, and
7 disclosure of Plaintiffs’ Protected Personal Information.

8 140. As a direct and proximate result of Money Transfer Defendants’ and
9 the Database Defendant’s unauthorized disclosure of Protected Personal
10 Information, Plaintiffs were injured and suffered violation of statutory privacy
11 interests.

12 141. In accordance with Cal. Civ. Code § 1798.150(b), prior to initiating this
13 suit, Plaintiffs’ counsel served Money Transfer Defendants and the Database
14 Defendant with proper notice of these CCPA violation via Federal Express.

15 142. Plaintiffs seek actual damages, statutory damages, costs, injunctive
16 relief, and attorney’s fees.

17 **COUNT 2**

18 **Invasion of Privacy Under California Constitution Art. 1, § 1**
19 **(On behalf of Plaintiffs, the Class, and Subclass against All Defendants)**

20 143. Plaintiffs incorporate the foregoing paragraphs as if set forth fully
21 herein.

22 144. Plaintiffs bring this count individually and on behalf of the members of
23 the Class and Subclass against the Money Transfer Defendants and Database
24 Defendant.

25 145. Plaintiffs, Class members, and Subclass members had a reasonable
26 expectation of privacy in the Protected Personal Information that Money Transfer
27 Defendants and Database Defendant disclosed without authorization.

1 146. Plaintiffs, Class members, and Subclass members have a strong interest
2 in: (1) precluding the dissemination or misuse of their sensitive Protected Personal
3 Information and related data; and (2) making personal decisions regarding the use
4 of their Protected Personal Information and related data, including the right to know
5 how such data may be used and to whom such data may be sent.

6 147. Money Transfer Defendants and the Database Defendant wrongfully
7 intruded upon Plaintiffs', Class members', and Subclass members' seclusion in
8 violation of California law. Plaintiffs' and Class members reasonably expected that
9 the Protected Personal Information and related data that they entrusted to Money
10 Transfer Defendants would be kept private and secure and would not be disclosed
11 to any unauthorized third party or for any improper purpose.

12 148. Money Transfer Defendants and the Database Defendant intentionally
13 invaded Plaintiffs', Class members', and Subclass members' privacy rights under
14 the California Constitution by:

- 15 a. obtaining, storing, remitting, and disclosing remitting Plaintiffs',
16 Class members', and Subclass members' Protected Personal
17 Information and related data to TRAC and Forcepoint, both
18 unauthorized, undisclosed third parties;
- 19 b. obtaining, storing, remitting, and disclosing Plaintiffs', Class
20 members', and Subclass members' Protected Personal Information
21 and related data to unauthorized, undisclosed third parties, to wit:
22 law enforcement;
- 23 c. enabling the disclosure of Protected Personal Information and
24 related data about Plaintiffs, Class members, and Subclass
25 members in a manner highly offensive to a reasonable person; and
26
27
28

1 d. enabling the disclosure of Plaintiffs', Class members', and Subclass
2 members' Protected Personal Information and related data without
3 their informed, voluntary, affirmative, and clear consent.

4 149. A reasonable person would find it highly offensive that Money Transfer
5 Defendants and the Database Defendant intentionally remitted Plaintiffs', Class
6 members', and Subclass members' Protected Personal Information and related data
7 to TRAC, Forcepoint, or any unauthorized third party without notice or consent to
8 do so.

9 150. Plaintiffs, Class members, and Subclass members did not consent to
10 any of Money Transfer Defendants' and the Database Defendant's alleged
11 misconduct, including any transfer or remittance of Plaintiffs', Class members', and
12 Subclass members' Protected Personal Information to TRAC or Forcepoint,
13 unauthorized and undisclosed third parties, or to any party thereafter following
14 Money Transfer Defendants' improper disclosures to TRAC and/or Forcepoint.

15 151. Money Transfer Defendants and the Database Defendant acted
16 knowingly or in reckless disregard of the fact that a reasonable person in Plaintiffs',
17 Class members', and Subclass members' position would consider all Defendants'
18 actions highly offensive.

19 152. Money Transfer Defendants and the Database Defendant were aware
20 that they were disclosing, transferring, or remitting Protected Personal Information
21 to unauthorized, undisclosed third parties and that doing so was not in response to a
22 lawful legal request.

23 153. Money Transfer Defendants' and the Database Defendant's unlawful
24 invasions of privacy damaged Plaintiffs and Class members. As a direct and
25 proximate result of these invasions, Plaintiffs, Class members, and Subclass
26 members suffered mental distress, and their reasonable expectations of privacy were
27 frustrated and defeated.

1 154. This invasion of privacy is serious in nature, scope, and impact.

2 155. This invasion of privacy constitutes an egregious breach of social
3 norms underlying the right to privacy.

4 156. Plaintiffs, Class members, and Subclass members therefore seek all
5 relief available for such invasion of privacy in violation of Article 1, § 1 of
6 California's Constitution.

7 **PRAYER FOR RELIEF**

8 Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, Bertha Meza, Griselda Aviles
9 Carrillo, and Jose Gerardo Vallejo Perez individually and on behalf of all others
10 similarly situated, respectfully request that this Court enter an Order:

11 a) Certifying the Class under Rule 23 and naming the aforementioned
12 Plaintiffs as representatives of the Class and respective Subclasses and Plaintiffs'
13 attorneys as Class Counsel;

14 b) Declaring that Money Transfer Defendants' and Database Defendant's
15 conduct violates the laws and standards referenced above;

16 c) Finding in favor of Plaintiffs, the Class, and Subclass on all counts
17 asserted herein;

18 d) Enjoining Money Transfer Defendants and Database Defendant from
19 continuing to provide access to or copies of Plaintiffs', Class members', or Subclass
20 members Protected Personal Information, or otherwise not complying with the
21 CCPA.

22 e) Awarding Plaintiffs, Class members, and Subclass members statutory
23 damages for each violation of the CCPA;

24 f) Awarding Plaintiffs, Class members, and Subclass members actual
25 damages for each violation of the CCPA;

26 g) Awarding Plaintiffs, the Class, and the Subclass their reasonable
27

1 attorney's fees, expenses, and cost of suit;

2 h) Awarding pre- and post-judgment interest, to the extent allowable;

3 i) Requiring further injunctive and/or declaratory relief as necessary to
4 protect the interests of Plaintiffs and the Class; and

5 j) Awarding such other and further relief as equity and justice require.

6 **JURY DEMAND**

7 Plaintiffs request a trial by jury of all claims that can be so tried.

8 Dated: April 12, 2024

Respectfully submitted,

9
10 By: /s/ Taras Kick

11 Taras Kick (Cal. Bar No. 143379)

12 taras@kicklawfirm.com

13 Tyler Dosaj (Cal. Bar No. 306938)

tyler@kicklawfirm.com

14 **THE KICK LAW FIRM, APC**

815 Moraga Drive

15 Los Angeles, CA 90049

16 Tele: (310)395-2988

17 Fax: (310)395-2088

18 Daniel H. Charest (*pro hac vice*)

19 dcharest@burnscharest.com

20 Darren Nicholson (*pro hac vice*)

dnicholson@burnscharest.com

21 Chase Hilton (*pro hac vice*)

chilton@burnscharest.com

22 **BURNS CHAREST, LLP**

900 Jackson Street, Suite 500

23 Dallas, TX 75202

24 Tele: (469)904-4550

25 Fax: (469)444-5002